1116-12-773 **Tamalika Mukherjee*** (txm1809@rit.edu). *Homomorphic Encryption: Ring Learning With Errors.*

Homomorphic Encryption (HE), sometimes considered the "Holy Grail of Cryptography", is a method of performing calculations on encrypted data. Fully Homomorphic Encryption (FHE) schemes can perform an arbitrary number of additions and multiplications but are currently practically inefficient to implement for industry standards. On the other hand, Somewhat Homomorphic Encryption (SWHE) schemes can perform a limited number of multiplications on encrypted data and are much more efficient. Some SWHE schemes are based on the Ring Learning With Errors (Ring-LWE) security assumption, we will present one such scheme based on the scheme developed by Brakerski and Vaikuntanathan. The Ring-LWE assumption holds for $\mathbb{Z}[x]$ modulo any cyclotomic polynomial, we will explore the properties of the cyclotomic polynomial used in our scheme as well as the experiments that we performed on it. (Received September 12, 2015)